OUR SHARED RESPONSIBILITY · OCTOBER 2010 ·

NATIONAL CYBERSECURITY AWARENESS MONTH

If You Suspect Malware Is On Your Computer...

The following behaviors are signs your computer may be infected with malware:

- Computer slows down, malfunctions, or displays repeated error messages
- Computer won't shut down or restart
- Computer serves up a lot of pop-up ads, or displays them when you're not surfing the web
- Computer displays web pages or programs you didn't intend to use, or sends emails you didn't write

If you notice any of these behaviors, follow the steps detailed below:

1) Stop shopping, banking, and other online activities that involve user names, passwords, or other sensitive information.
   - As soon as possible, use an uninfected computer to change all of your online passwords.

2) Confirm that your security software is active and current: at the bare minimum, your computer should have anti-virus and anti-spyware software, and a firewall.
   - You can buy stand-alone programs for each element—or a security "suite" that includes these programs—from a variety of sources, including commercial vendors or from your Internet Service Provider. Security software that comes pre-installed on a computer generally works for a short time unless you pay a subscription fee to keep it in effect. In any case, security software protects against the newest threats only if it is up-to-date. That's why it is critical to set your security software and operating system (like Windows or Apple's OS) to update automatically.
   - Be aware that some scam artists distribute malware disguised as anti-spyware software. Resist buying software in response to unexpected pop-up messages or emails, especially ads that claim to have scanned your computer and detected malware. That's a tactic scammers have used to spread

King County
Information
TECHNOLOGY

Chief Information Security and Privacy Officer
Ralph Johnson ~ 206-263-7891

malware, and that has attracted the attention of the Federal Trade Commission, the nation's consumer protection agency, as well as a number of state law enforcement agencies.

3) Once you confirm that your security software is up-to-date, run it to scan your computer for viruses and spyware.
   - Delete everything the program identifies as a problem. You may have to restart your computer for the changes to take effect.
   - If you suspect that your computer still is infected, you may want to run a second anti-spyware or anti-virus program. Some computer security experts recommend installing one program for real-time protection, and another for periodic scans of your machine as a way to stop malware that might have slipped past the first program.

4) If the problem persists after you exhaust your own ability to diagnose and treat it, you should seek an expert's assistance.
   - Some users have found it helpful to visit online forums that focus on malware investigation and removal. These forums provide a way to connect with IT professionals and knowledgeable volunteers. Please note that Google is not affiliated with these sites, and cannot guarantee the accuracy or effectiveness of any advice offered in them. However, some users have found the information and assistance provided there to be helpful.
   - If your computer is covered by a warranty that offers free tech support, contact the manufacturer. Before you call, write down the model and serial number of your computer, the name of any software you've installed, and a short description of the problem. Your notes will help you give an accurate description to the technician.
   - If you need professional help, if your machine isn't covered by a warranty, or if your security software isn't doing the job properly, you may need to pay for technical support. Many companies—including some affiliated with retail stores—offer tech support via the phone, online, at their store, or in your home. Telephone or online help generally are the least expensive ways to access support services—especially if there's a toll-free helpline—but you may have to do some of the work yourself. Taking your computer to a store

usually is less expensive than hiring a technician or repair person to come into your home.

5) Once your computer is back up and running think about how malware could have been downloaded to your machine, and what you could do to avoid it in the future.
    - If your security software or operating system was out-of-date, download the newest version and set it to update automatically. Use the opportunity to backup important files by copying them onto a removable disc.
    - Be sure to change any online passwords that you used while your computer was infected.

6) Finally, monitor your computer for unusual behavior.
    - If you suspect your machine has been exposed to malware, take action immediately. Report problems with malware to the FTC and to your ISP so it can try to prevent similar problems and alert other subscribers.